Secure Software Agents and Agent-based Security Systems

Steven Y. Goldsmith, DMTS
Distributed Systems Assurance Research

AISL
advanced information systems laboratory

Sandia National Laboratories

History: Engineered Collectives Grand Challenge

- Challenge: ***How can we design large collections of cooperating entities to solve real-world problems with predictable behavior? What problems can be solved only this way?***
- Answer: **Intelligent Agents**
- Primary problem addressed: The malicious insider security problem

Defeating Malicious Insiders

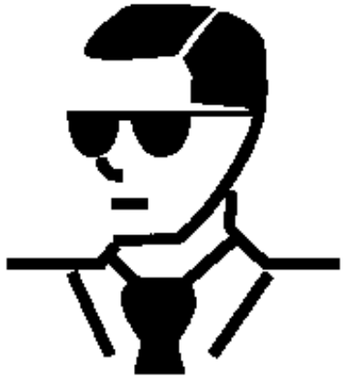
Today's information security approaches are failing against the modern cyber-threat.

Information security features are implemented hierarchically (e.g. system administration functions, intrusion detection systems, PKI cryptography, "need-to-know" products)

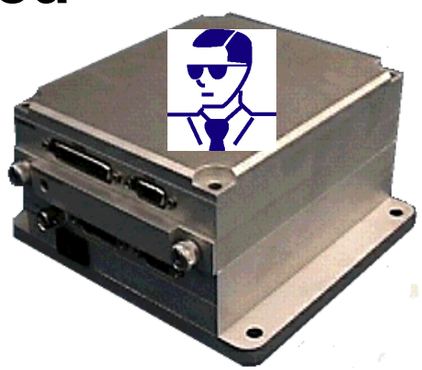
- **Significant vulnerability to insider threat**
- **Single points of failure and opportunity to adversaries**
- **Difficult to scale**

Challenge: provide high security *and* high functionality to users, without trading them off against each other.

What is an Agent?



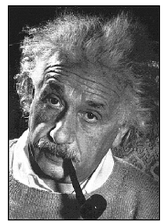
- A computer program
- Adheres to certain architectural constraints
- Incorporates particular concepts and technologies
  - Distributed
  - Knowledge-based



Intelligent Agent Attributes

These "Heavyweight" Agents are:

Reactive



Proactive/Deliberative

Autonomous

Adaptive

Mobile

Secure*

Social

Autonomy

- Operate without significant human intervention
- Maintains self-integrity
- Evaluates requests and elects to respond
  - Agent lifecycle
  - Long-lived agents

Reactivity

- Respond to stimuli from the environment
- Determine responses by simple pattern recognition
  - Limited by the lack of domain modeling
  - Minimal historical information

Proactivity

- Pursue normative goals
- Initiate processes and actions of their own volition
- Deliberate before acting using internal models of the environment
  - Motivated agents
  - Knowledge-based agents

Social Ability

- Communicate with other agents
- Collaborate to solve problems
- Strive to maintain collective states
  - Shared knowledge
  - Communicative acts

Adaptation

- Alter behaviors in response to changing environments
- Learn new situation-response patterns
  - Reactive agents

Learning

- Alter their internal models
- Add new knowledge
- Create new goals

  - Proactive/Deliberative Agents

Mobility

- Move code the network to perform computation
  - Mobile code
  - Mobile agents

What is a Collective?

Secure Agent Collective:

Secure software agents organized into a security architecture that significantly improves the security of the distributed information system of which they are part, even against malicious insiders.

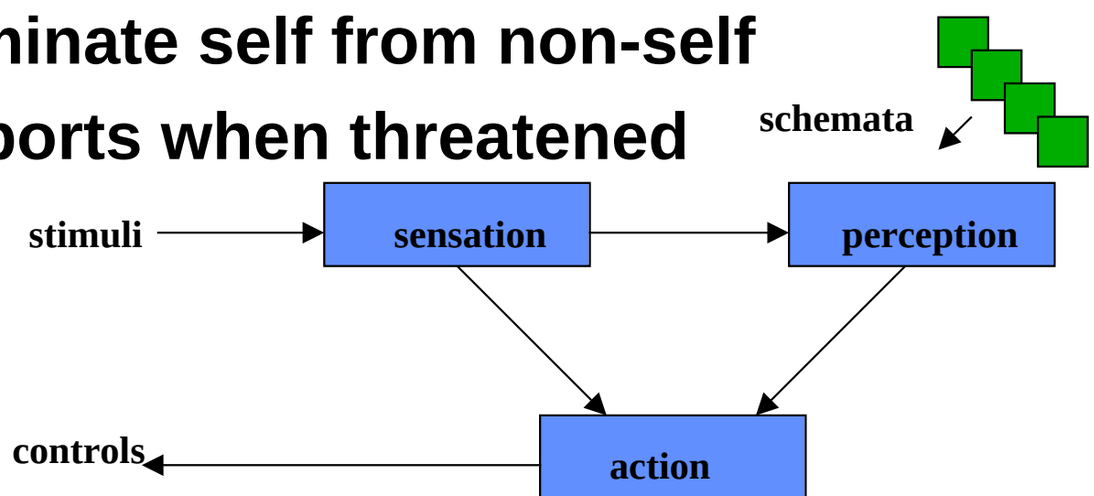
The Secure Agent Collective Provides:

- Strong security at the application layer
- Security that also reaches down into the Operating System
- Invisible management of security for the user
- Distribution of the trust in the system
- Explicit security policy, enforced by secure processes

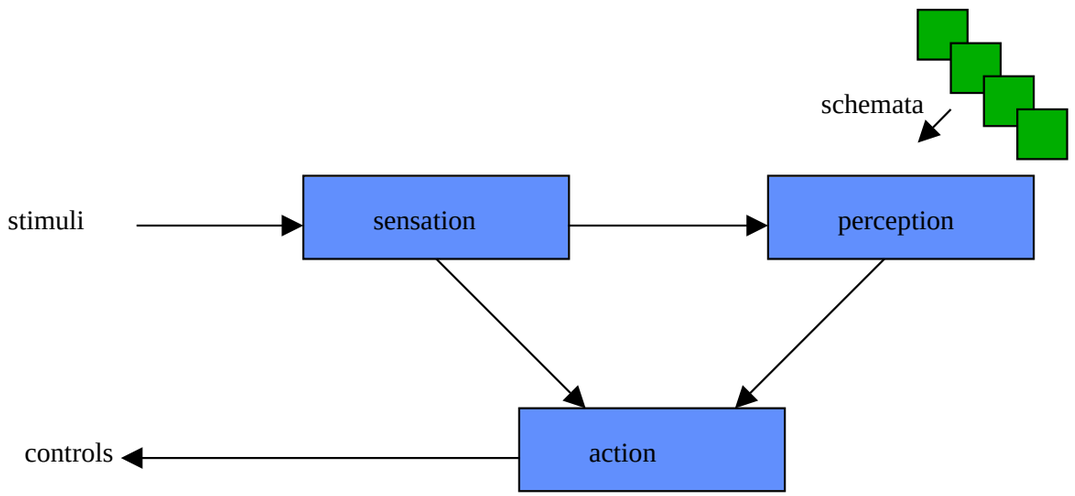
Our Agents Are Designed to Be Suspicious of Their Environment

Strong security at the application layer...

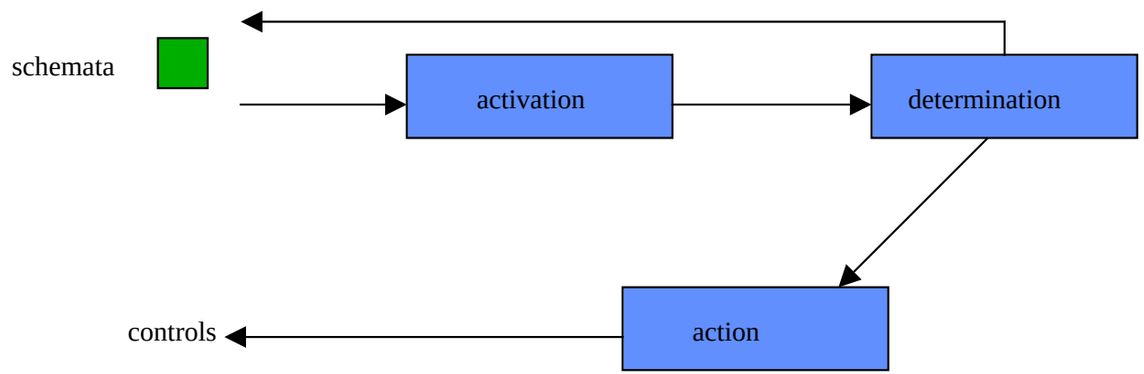
- They identify packet and stream patterns prior to service dispatch
- They rapidly classify unusual data streams--much more rapidly than people
- They require authentication for many data streams
- They can discriminate self from non-self
- They can close ports when threatened



Reactive Component

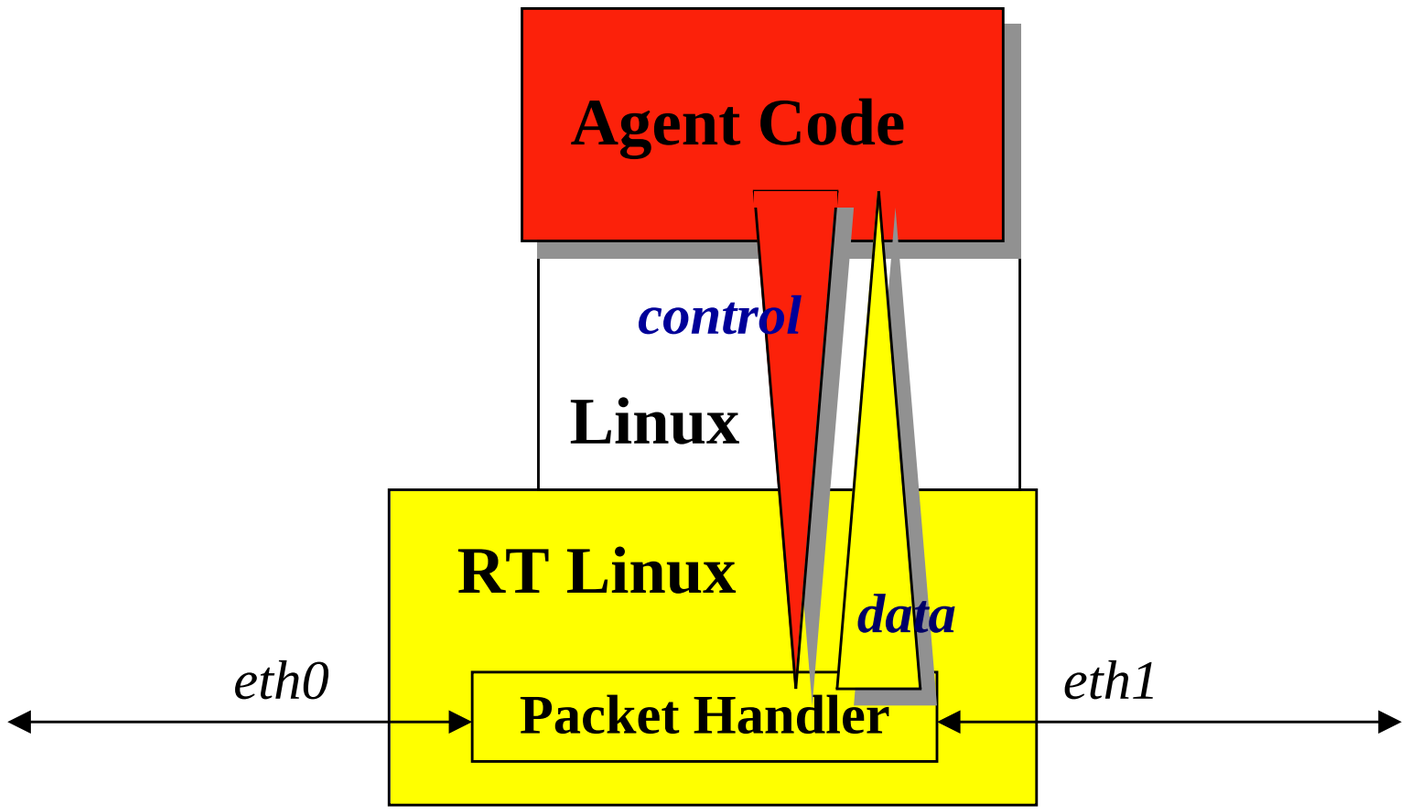


Deliberative Component



Integration of Real-time Linux Enhances the Agent's Efficacy

Security that reaches down into the OS



Red Teaming Is a Critical Part of the Development Process and a Metric of Success

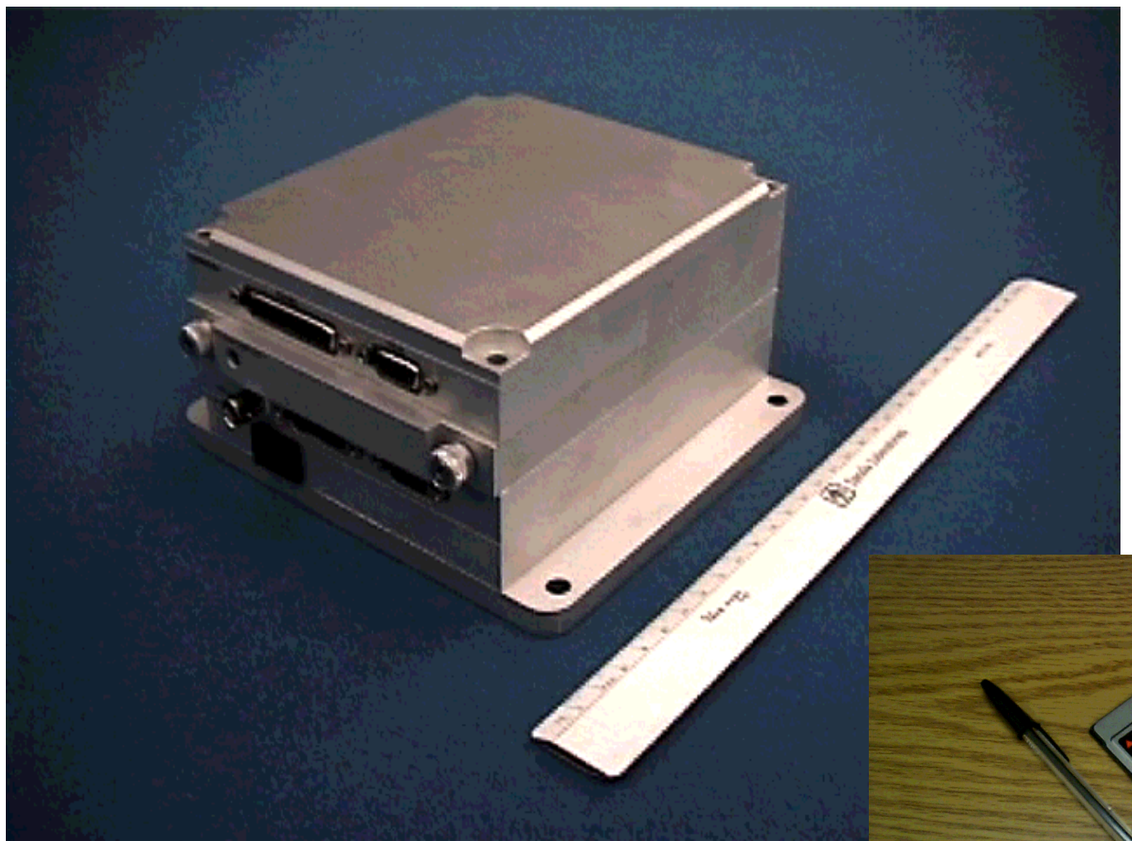
We Red Teamed our Secure Agents Model...

- **First Red Team exercise completed 2QFY00:**
  - **Red team did not halt any agent process nor damage or acquire any designated document**
  - **Agents detected port scans, floods, and unauthenticated messages and communicated this to one another**
  - **Agents selectively discarded unexpected inputs**
- **Second Red Team exercise completed 4QFY00:**
  - **System demonstrated protection against malicious insider challenges**
  - **Protocol and other problems identified by Red Team were repaired within hours**

Our Experiments Have Demonstrated the Capabilities Of Our Agent Collectives

- Agents perform missions not possible by other means
- Agents protect themselves from attacks
- Agents monitor networks for security
- Agents enforce security policies
- Agents cooperate with administrators
- Agents collaborate to protect networks
- (Agents attack adversaries)
- (Agents perform vulnerability analyses)

Embedded Secure Network Agent

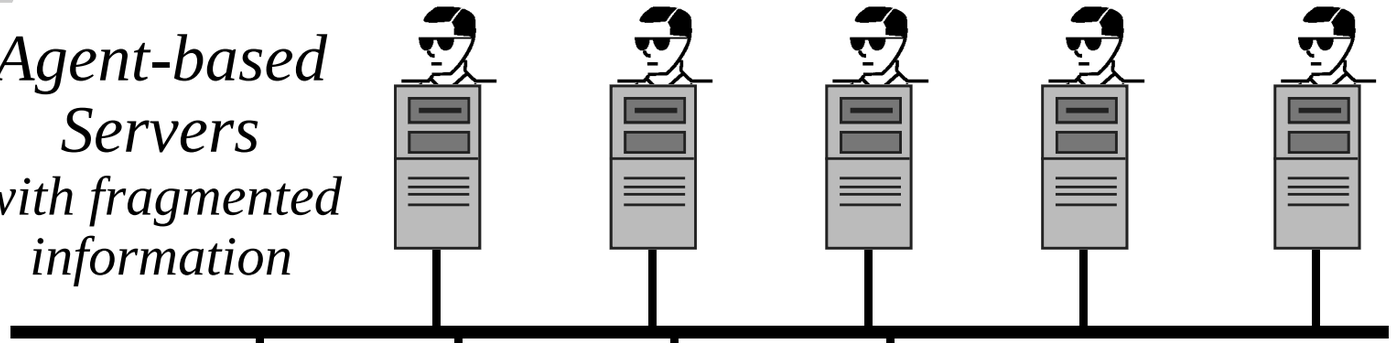


Agent-in-a-Box

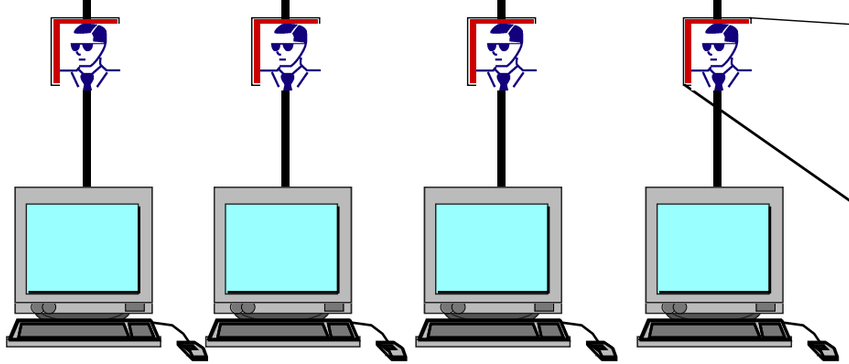
Agent-on-a-Stick

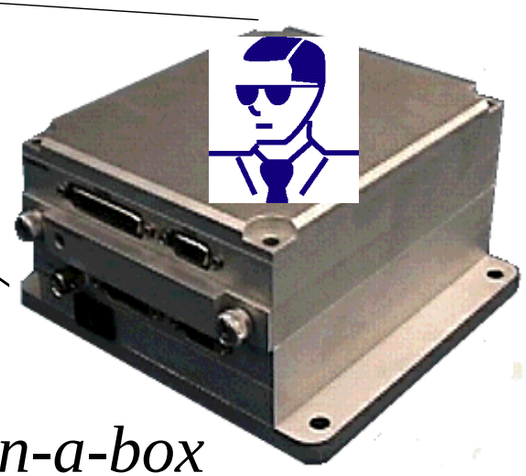
Operational Concept: Agent-Mediated Access

Agent-based Servers
with fragmented information



Thin User Clients

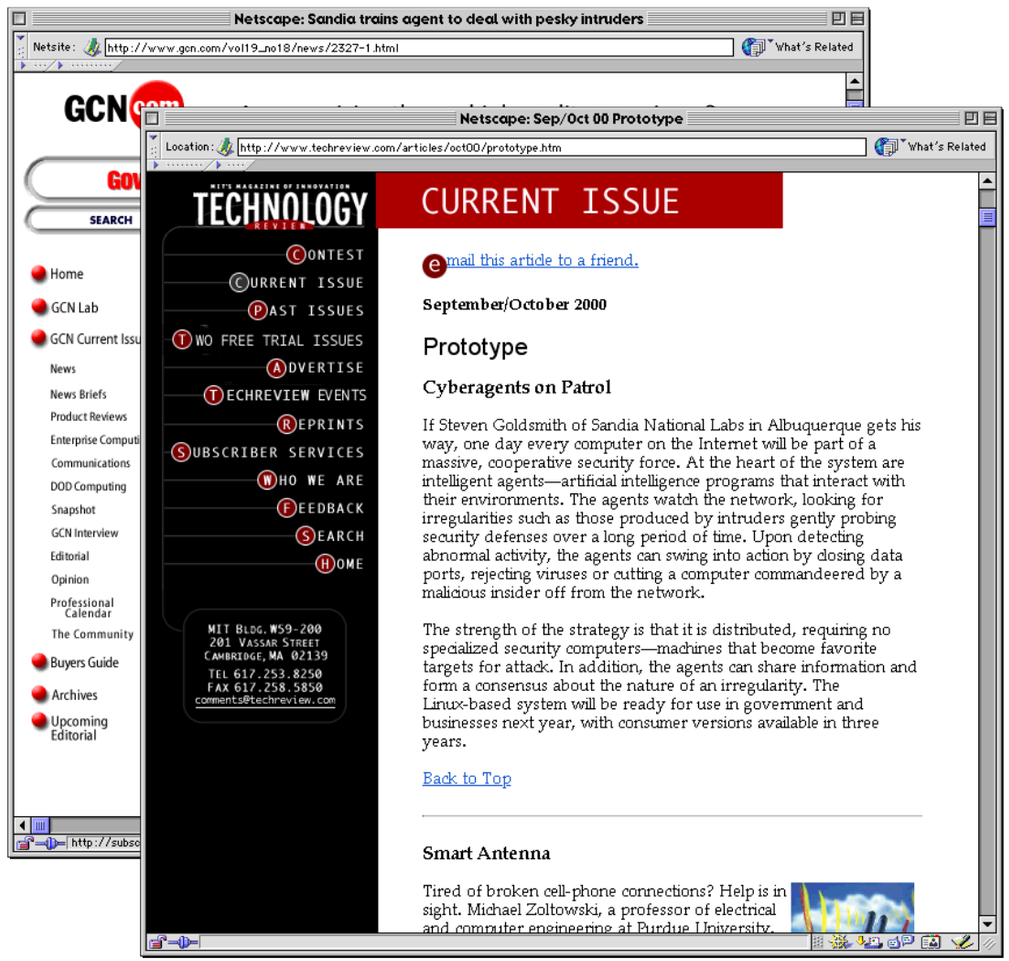




Agent-in-a-box

External Recognition

- Scientific American (12/2000)
- MIT Technology Review (10/2000)
- Albuquerque Journal
- Focus (7/26/2000)
- Red Herring (11/2000)
- Business 2.0 (9/28/2000)
- Government Computing News
- Beyond 2000
- ***...many others***



Hypotheses Validated

- Iterative *red-teaming* is essential to the research.
- Security must be a *fundamental* requirement in the initial development of the agent architecture.
- Forcing the adversary to incur the cost of Class III attacks is essential. We can defend against Class I and Class II attacks.
- Agents can provide unprecedented security together with extraordinary functionality.
- This systems approach has extraordinary promise.